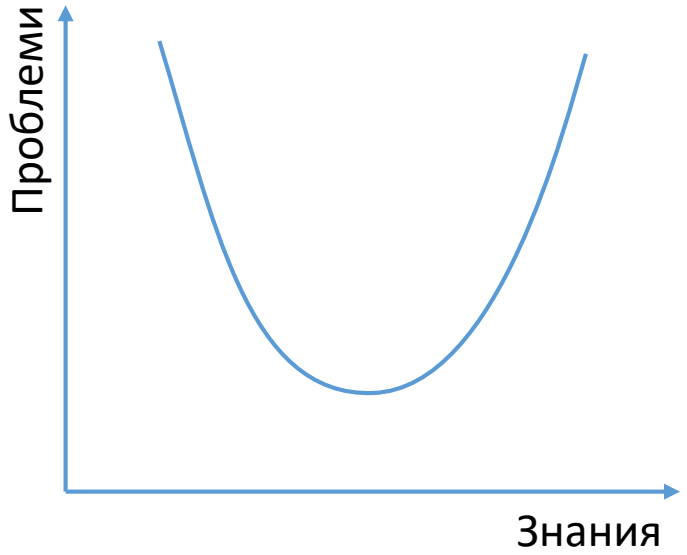
Администриране на потребители и потребителски групи

ас. Стоян Мечев
катедра „Информационни технологии“
ВВМУ „Н. Й. Вапцаров“

Общо за администрирането

- В какво се състои работата на системния администратор:
  - инсталиране и конфигуриране на операционната система;
  - инсталиране на периферни устройства;
  - поддръжка на системата;
    - проверка на журнални файлове и изтриване на стари такива;
    - архивиране на данни;
    - инсталиране на нов софтуер и обновяване на стар;
    - реагиране на промени – нови потребители, нова периферия и др.



- root акаунта (super user)
  - Специални права за системния администратор
    - почти неограничен достъп до всички ресурси на системата – данни, устройства и компоненти на системата;
    - възможност да прави промени, каквито никой друг потребител на системата не може да направи;
    - съответно, възможност да направи големи бели => използвайте root акаунт само при необходимост. През останалото време работете като обикновен потребител – проследяемост.
- **soft skills (communication skills) 50% от работата**
  - необходими при налагане на фирмени политики;
  - използвайте всяка възможност за да ги развивате;
  - не съм попадал на специална дисциплина в учебната програма;
  - отговорно поведение.

Инструменти за системно администриране

- Има инструменти за администриране в графична среда, специфични на конкретната дистрибуция.
- YaST инструмент за SUSE Linux.
- Webmin – всеки, който има браузър може да се опита да администрира системата.
- В крайна сметка, минусите са повече от плюсовете:
  - Администраторът става зависим от дистрибуцията, с която работи.
  - Предоставя се лесна възможност за администриране и така може да работят хора, които не знаят съвсем добре, какво правят – например при конфигуриране на firewall.
  - Обикновено са трудно „преносими“ – ако трябва да се направят настройки на няколко компютъра, е по-добре да се напише скрипт, който да свърши нещата, отколкото да се задават настройки на всеки компютър по отделно.
  - Не осигуряват всички възможности, които дава командния ред.

Системно администриране - потребители.

- Защо изобщо е необходимо ползването на потребители?
  - Потребителите имат работни директории и могат да задават права за достъп върху собствените си файлове (chmod).
  - Предпазва системата от вредни въздействия от страна на некомпетентни потребители (например случайно да изключат компютъра или общ хардуер, като мрежова карта например.
  - Потребителите могат да бъдат обединявани в групи, на които да се задават отделни специални права.
  - Linux разграничава акаунти, не потребители. Може един потребител да има няколко акаунта с различно предназначение - например може да има акаунт само за сърфиране.
- Всеки потребител, освен потребителско име има и номер **User ID** или **UID**.
  - Ядрото работи с UID, а не с потребителското име - всички процеси, собственост на файлове са свързани с UID.
  - При изтриване на потребител, неговият UID може да се прехвърли и така ще се прехвърлят и правата върху файловете.
  - Може един и същи UID да се присъедини да два различни потребителя. Тогава те ще имат еднакви права и достъп до ресурсите на системата.

Системно администриране - групи.

- Потребителите могат да бъдат обединявани в групи, на които да се задават отделни специални права.
- Всеки потребител участва в една основна група и (евентуално) в няколко вторични.
  - Във версии на ядрото до 2.4 включително, потребител може да бъде член най-много на 32 допълнителни групи. След версия 2.6 това ограничение отпада.
- Всяка група има ID (Group ID или GID)
- **id** - информация за ID на потребителя
- **id** -Gn
- **id** ivan
- **last** - справка на последните логвания
- **groups** [username]
- **chmod** o-r /var/log/wtmp

  $ last

  last: cannot open /var/log/wtmp: Отказан достъп

Работа с root права.

- **Работа с root права**
  - Ако влезете като root в графична среща, след това всички приложения, които се стартират, имат такива права.
  - Във файла **/etc/securetty** има списък на всички терминали, от които можете да влезете като **root**.
  - **su** – стартира отделен шел, в който работите като **root**. *С тази команда можете да работите от името на всеки потребител.*
  - Някои дистрибуции, например Ubuntu, изобщо не позволяват влизане като **root**. Използва се **sudo <command>**. Такива права се дават по подразбиране на първия създаден потребител.
  - Обикновено се различава по подканващото съобщение на шел **$** или **#**.
  - По-добре малко администратори, от колкото много.
  - Който не работи, той не греши.

Псевдо-потребители

- Концепцията за потребители и потребителски групи се използва за задаване на права за достъп до отделни части от системата на вътрешни административни функции.
- Файловете
  - /etc/passwd
  - /etc/group

Съдържат информация за псевдо потребители

- **cut -f 1-4 -d: /etc/passwd|tr ':' '\t',**

- root привилегиите са свързани към UID 0
- Тези акаунти могат да бъдат достъпвани с командата **su**.
- Могат да се използват като собственици на файлове или директории за да контролират достъпа до тях.

Файлът /etc/passwd

- Представлява база данни съдържаща потребителите на системата.
- Структура:
  - <user name>:<password>:<UID>:<GID>:<GECOS>:<home directory>:<shell>
    - $ cut -f 1,6,7 -d: /etc/passwd|tr ':' '\t'
  - **<user name>** – малки букви и цифри, започва с буква. Внимание, някои UNIX системи ползват само първите 8 символа.
  - **<password>** – традиционно, това поле съдържа криптираната парола на потребителя. Съвременните версии на Линукс използват файл /etc/shadow, който е с ограничен достъп, а в /etc/passwd в това поле има знак x.
  - **<UID>** число (от 0 до 2^{32}–1), което показва номера на потребителя:
    - 0 до 99 запазени за системата;
    - 100 до 499 запазени за псевдо-потребители на софтуерни пакети;
    - от 500 (или 1000) нагоре, започват реални потребители.
  - **<GID>** ID на основната група на потребителя. Всеки потребител принадлежи най-малко към една група.
    - Някои дистрибуции имат група наречена users, която е обща за всички потребители.
    - Други дистрибуции, (Red Hat, Debian) създават група със същото ID, като потребителското.
    - cut -f 1,3,4 -d: /etc/passwd|tr ':' '\t'|sort -k 2 -h
    - Информация за вторичните групи се съдържа във файла /etc/groups
  - **<GECOS>** "General Electric Comprehensive Operating System" – съдържа допълнителна информация за потребителя, като истинско име, телефон и т.н. Изпробвайте командата **chfn**.
  - **<home directory>** основна работна директория на съответния потребител.
  - **<shell>** командния интерпретатор, който се стартира при логване на потребителя.
    - може да се променя с командата **chsh**; списъкът на шеловете е във файла: /etc/shells

***Полетата в червено са задължителни.**

Файлът /etc/shadow

- Съхранява криптираните пароли.
- Структура:
  - <user name>:<password>:<change>:<min>:<max>:<warn>:<grace>:<lock>:<reserved>
  - <user name> – отговаря на user name в /etc/passwd
  - <password> – криптираната парола. Може да е празно. Ако има * или ! акаунтът е заключен;
  - <min> – минимален брой дни, след посленатa смяна на паролата, за да може да бъде сменена отново;
  - <max> – максимален брой дни, в които паролата остава валидна. След това трябва да я смени.
  - <warn> – брой дни преди <max> от които да почне предупреждаване за смяна на паролата.
  - <grace> – брой дни след <max>, след което акаунта се заключва, ако не смени паролата.
  - <lock> – датата, в която акаутът ще бъде заключен, отново в дни, считано от 01.01.1970.
- Криптиране.
  - Осемзначна парола $6.6*10^{15}$
  - Криптира се пробната парола и се сранява с тази, която проверяваме;
  - Системата добавя случаен „сол“ – една от 4096 възможности;
    - Алгоритъмът MD5 добавя 48 битова „сол“.
  - Не разчитайте много на допълнителните полета;
  - Социалното инженерство е много по-опасно от грубата сила.

Файлът /etc/group

- Съхранява информация за групите.
- Структура:
  - <group name>:<password>:<GID>:<members>
  - <group name> – име на групата;
  - <password> – допълнителна парола за групата; “*” смяната на група.
  - <GID> – ID на групата;
  - <members> – списък на членовете на групата, разделени със запетая, за които групата се явява вторична група.
- Има файл /etc/gshadow
  - подобен на /etc/shadow
  - допълнително съдържа информация за администраторите на групата

Команди getent, useradd, adduser

- **getent** – пълната информация за конкретен потребител от различни източници.
  - getent passwd ivan
- **useradd** [options]<user name> създаване на потребител. Може изцяло да се изпълни ръчно. За Debian се препоръчва да се ползва “adduser”.
  - c <comment> данни за полето GECOS
  - d <home directory> ако е празно се ползва /home/username
  - e <date> на тази дата акаунтът ще бъде деактивиран (YYYY-MM-DD)
  - g <group> име на група или GID на основната група. Необходимо е групата да съществува.
  - G <group>[,<group>] списък на вторичните групи. Необходимо е групите да съществуват.
  - s <shell> – логин шел за потребителя.
  - u <UID> – UID на новия потребител. Трябва да е уникален. Може да се използва съществуващ с опция „-o“
  - m създава home директория и копира набор от файлове. Файловете идват от /etc/skel
  - акаунтът се активира след задаване на парола за потребителя.

Команди passwd, chage

- Задаване на парола за потребител: **passwd**. Потребителите могат да сменят своите пароли.
  - **passwd** ivan
  - passwd -S ivan - статус на ivan (P или PS - има парола; L или LK - заключен; NP - няма парола), дата на последна промяна, min, max

  -l заключва акаунта;

  -u отключва акаунта;

  -n 7 смяна на паролата най-късно след 7 дни;

  -x 30 смяна на паролата най-малко на всеки 30 дни;

  -w 3 период grace 3 дни.
- Промяна другите параметри във файла passwd - команда **chage**:
  - **chage ivan** - диалогов режим за задаване на данни за потребител ivan
  - chage -E 2019-12-01 ivan - заключва акаунта на ivan от 01.12.2019г.

Команди userdel, usermod, vipw

- Изтриване на потребителски акаунт: **userdel**. Изтрива записите в различни файлове и работната папка. Може всичко да се направи ръчно.
  - **userdel** [-r] ivan - изтрива акаунта на потребител ivan. Опцията „-r" подсигурява изтриването на работната директория и /var/mail/ за съответния потребител;
  - **find** / -uid <UID> -delete намира и изтрива всички файлове свързани с този потребител.
- Промяна на потребителски акаунт и принадлежност към група: **usermod**. Пак може ръчно, чрез редактиране на /etc/passwd и /etc/group.
  - **usermod** -g <group> <user name> - сменя основната група на потребителя;
  - Внимавайте, ако сменяте UID, да се смени и собствеността на файловете! Защо?
  - Приема същите параметри като **useradd**.
- Редактиране на информация за потребител директно: **vipw**. Стартира текстов редактор (обикновено vi) и отваря файла /etc/passwd, като го заключва за други потребители.
  - с опиция „-s" отваря файла /etc/shadow.

Команди groupadd, groupmod, groupdel, vigr.

- Създаване на група: **groupadd** . Може всичко да се направи ръчно, чрез редактиране на файлове /etc/group и /etc/gshadow.
  - **groupadd** [-g <GID>] <group name>
  - -g - позволява да се зададе ID на групата. Първите 99 ID обикновено са запазени за системни групи.
- Редактиране на група: **groupmod**. Пак може ръчно.
  - **groupmod** [-g <GID>] [-n <name>] <group name>
  - [-g <GID>] - сменя ID на групата;
  - [-n <name>] - сменя името на групата, без да сменя GID;
- Изтриване на група: **groupdel**. Изтрива група.
  - **groupdel** <group name>
  - Основна група на потребител не може да бъде изтрита. Ако се налага изтриване, първо се определя нова основна група с **chgrp**.
- Администриране на група: **gpasswd**. Супер-потребителя може определи администратор на групата. Администраторът на група също може да изпълнява командата **gpasswd**.
  - **gpasswd** -A <user>,... <group> - определя администратори на групата;
  - **gpasswd** -a <user> <group> - добавя потребителя към групата;
  - **gpasswd** -d <user> <group> - премахва потребител от групата.
- Редактиране на данните за група **vigr** и **vigr -s**. Командите работят аналогично на **vipw**.

Примери

```
useradd ivan.surf
```

```
# id ivan.surf
uid=1002(ivan.surf) gid=1002(ivan.surf) групи=1002(ivan.surf)
```

```
# adduser ivan.mail
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX configuration variable.  Use the `--force-badname'
option to relax this check or reconfigure NAME_REGEX.
```

```
# adduser stoyan1
Adding user 'stoyan1' ...
Adding new group 'stoyan1' (1003) ...
Adding new user 'stoyan1' (1003) with group `stoyan1' ...
Creating home directory '/home/stoyan1' ...
Copying files from '/etc/skel' ...
```

```
# adduser ivan.mail
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX configuration variable.  Use the `--force-badname'
option to relax this check or reconfigure NAME_REGEX.
```

```
# cut -f 1,2 -d: /etc/shadow|tr ':' '\t'|grep ivan
ivan    $6$Cz.lODiI$eFYnpkB/jz0v9x.EKlvble6nY729eUSGBxiug1fA4pkjpSrP/iWapwE8Kz1bHuC76QnKQzrTREZnyImPiKfA7/
ivan.surf       !
```

```
 passwd -S ivan.surf
ivan.surf L 02/25/2019 0 99999 7 -1
```

Благодаря за вниманието!

Въпроси?